ON-PREMISE FILE SERVER VS CLOUD STORAGE WITH INCIDENT MANAGEMENT: A COMPARATIVE STUDY

Jaymie Rae Medina[1] and Jennalyn Mindoro[2]

[1]Graduate Studies, Technological Institute of the Philippines, Manila, Philippines
[2]Computer Engineering Department, Technological Institute of the Philippines, Manila, Philippines

ABSTRACT

Many organizations are already shifting their infrastructure and applications to the cloud. Cloud technology is accessing and availing products and services over the internet. The maintenance of cloud technology is often managed by a cloud service provider. A comparison has been made between an existing technology, on-premise file servers, and virtualized file servers in the form of cloud storage to determine the advantages and disadvantages of each file-sharing system's performance. An architectural framework and a simulation of the new cloud storage architecture have been conducted to serve as file storage.

Finally, several users that are currently employing the existing on-premise file server technology have participated in user acceptance testing to try the cloud-based storage as a replacement for the file server. The test outcomes proved that end-users were able to execute their regular duties using cloud storage and that they favored it over their current file storage.

KEYWORDS

Storage, Cloud, On-premise, Incident Management, Server, AWS

1. INTRODUCTION

In recent years, things have rapidly changed due to the global pandemic situation. Changes in information technology and computing systems need to be recognized by any organization and force them to move into the next generation of computing which is known as a paradigm shift [1]. Due to the recent COVID-19 pandemic, companies need to have a business continuity plan to continue delivering products and services despite the situation and the government announcement of a nationwide lockdown [2]. Employees are forced to continue working from home and sustain the expected deliverables. Companies went from fully occupied offices to skeletal staffing and later to a limited number of employees only reporting to the office physically. Employees have been migrated from desktops to laptops for the ability to work from home. Other physical devices that are essential for the company to function continuously, such as network switches, routers, access points, and servers, are all still sitting in the office and are accessed by the employees remotely.

One of the essential devices that the employees are required to access daily to perform day-to-day tasks is the file server. A file server, or a file-sharing system, is one of the key devices that support employees in saving and sharing important documents across the company. Various

David C. Wyld et al. (Eds): IoTE, CNDC, ACITY, DPPR, AIAA, NLPTA, WEST, ICSS -2023
pp. 271-284, 2023. CS & IT - CSCP 2023 DOI: 10.5121/csit.2023.132221

documents such as images, PDF files, contracts, and client information are stored in a single repository for ease of access by the employees [3]. A file server also needs to be secured to protect confidential information stored within it. Since every employee is required to work remotely, a VPN connection is necessary to access the company resources. Even though the company finds it beneficial to access the company data in a single repository, even though these servers are physically available in the office, there are still some drawbacks experienced since the implementation of flexible working arrangements.

One of the technical drawbacks that the employees experience is that the connection is not stable. Employees experience latency and delay, especially when multiple users are accessing the server at the same time. Employees are unable to open the large files directly from the server, and the only workaround is to create a copy of the file from a local laptop to work on the file and put it back on the server once done. This causes a delay in doing daily work and too much of a hassle. If the employees will be working on hundreds of files, achieving the daily deliverable is a challenge. Another drawback is that due to the pandemic, the scalability of an on-premise server is limited and is often delayed.

If the storage capacity has been maximized, one of the solutions to resolve the problem is by upgrading the storage component, replacing the physical server, or migrating the server into a brand-new device, including the upgrade of software and hardware components which is very expensive. Based on the study, one of the major challenges for people working remotely mainly focuses on the technical issue [4].

Since there is limited staffing in most of the suppliers and vendors, upgrading the physical server was a challenge during the pandemic. Most of the suppliers receive materials from another supplier outside the country, and since the nearby borders were closed, materials needed were not delivered on time or not delivered at all. Maintaining the physical server would be a challenge as well for IT administrators and, at the same time, with vendors. A personal visit needs to be made in case they need to upgrade the hardware components. Most people did not risk their safety in traveling for work during the pandemic.

Alternatively, incident management is a way of handling incidents to avoid any disruption of a service provided by a system. An incident is a term used in the ITIL framework as any event that causes an interruption in service [5]. The main objective of incident management is to restore any interrupted service as quickly as possible and lessen the impact on the business. Incident management has different phases: incident detection, classification of incidents, investigation and diagnosis, resolution and recovery, and incident closure [6]. Incidents are prioritized based on urgency and business impact [5].

This study will focus on the comparison and benefits of both storage devices solving the technical challenges experienced by the employees of a company. The comparison can provide a solution to address the performance issues of the existing On-Prem storage approach. Automated incident management will also play an important role in achieving system reliability.

2. REVIEW ON RELATED LITERATURE

Over the years, several studies have been conducted to improve the file-sharing system efficiently and effectively. Some of the considerations from previous research are cost-efficiency, time-efficiency, high performance, and can be easily managed by IT administrators. Different approaches and procedures were used in each study, but the best method only varies concerning the scenario or challenges they wanted to resolve.

A recent study proposed a new method of peer-to-peer transfer using client-to-client file transfer protocol (C2CFTP) which proves that the new method is more efficient in terms of direct and indirect transfer [7]. The objective of the study is to reduce the file transfer delay in client-server-client communication. The methods the researchers used to improve the file transfer between two clients are direct and indirect transfer. Different services are used to implement a direct transfer, such as file push, blocking channel, and file pull. Alternatively, file push and file pull services are used in the indirect transfer. The results have been measured statistically by comparing the speed of file transmission using the block/non-block method and the direct/indirect method. The system has seen that with the use of the proposed method, the average file transmission time has decreased by 54%. The study concluded that using the indirect and direct transfer method would efficiently increase the performance of file transmission with decreased time delay and is capable of transferring large amounts of data over the network.

A study about file servers and the task management function that works with a cloud services platform for cost reduction has been conducted by Namee K. [8]. The researcher found that using a cloud-based platform alone to run the websites would be too expensive. The purpose of the study is to implement a technique for a web application to function on a cloud-based platform with the help of an on-premise file server. The researchers used Microsoft Azure as the cloud-based platform to run the website, Trello as the web-based application that creates a list of tasks created by the user, a file server that is used to store the files (.html), Microsoft To-Do is another web-based application that enables users to create tasks, and last is the Microsoft Planning which is another web application that enables a user to create tasks. In web design, the users have the choice of which web application platforms to use (Trell, Microsoft To-Do, or Microsoft Planning). Results show that users can access the website successfully after authentication has been made on Azure AD.

Data storage in cloud computing is critical in handling data security in terms of confidentiality, integrity, and availability. The main objective is to discuss possible security issues presented in the cloud environment and techniques on how to secure the data. Based on the research, to protect confidentiality, data needs to be encrypted. Data stored on a public cloud can be easily attacked internally and externally. Data integrity can be protected by using digital signatures to avoid unauthorized modification of data to maintain accuracy. By using these two mechanisms, the researchers can ensure that the data will remain available to be accessed by authorized users anytime and anywhere. To address data security in the cloud, a service-level agreement between the customer and the service provider should include and highlight an agreement for the confidentiality, integrity, and availability of data.

Another approach to improving file systems was conducted in a study by Liu et al. [9], where a new storage architecture has been studied/implemented and called FSP with the creation of a system prototype called DashFS (file system as a process). The main objective of this study is to improve the performance of storage systems while maintaining data quality and integrity. Different system frameworks already existed but had performance issues. Existing frameworks often use kernels when communicating with different processes which causes slowness (100 microseconds). Some existing frameworks do not involve kernels or minimally use kernels, but there are some security challenges. Using DashFS, file system operations are being supported by minimizing crash consistency and using a simple data structure. The system also improves the performance by reducing latency by 43%.

Incident management is a tool used in a water treatment facility to track down any unplanned service interruption, such as equipment breakdown, groundwater issues, and other unknown events [10]. In a recent study, the researchers developed an internet-based incident management tool to enable the operations communication center to monitor, communicate, and document

operation-related activities to provide a better service. A workflow diagram has been created for the entire process of identifying, categorizing, resolving, and closing incidents. A prototype has been created using ASP.net, SQL database, and SMS API. Results were gathered through user acceptance testing (UAT) questionnaires, and it has been shown that end-users have supported the system proposed.

Industries are rapidly shifting into a new generation of digital transformation, adopting a holistic approach towards new business models, reconstructing architectural designs, and reforming the products and services to establish continuous growth and the need for continuous improvement in supplying service offerings to customers and an improved relationship with partners and suppliers [11]. As quoted by a Greek philosopher, "Nothing is constant but change" also applies to the world of technology. Shifting into a new infrastructure towards the cloud has proven beneficial in recent studies.

Although public cloud storage has received tremendous growth over the past years, organizations are facing higher risks in cyber-attacks such as denial-of-service (DDoS), man-in-the-middle, phishing, password attacks, and many more. Billions in company revenue may be affected once they encounter data breaches. In a study by Kolevski et al., [12] three top companies in the United States (i.e., Sony, Anthem Healthcare, and Equifax) faced the risk of a data breach.

Since the pandemic, more and more companies are facing the risks of cyber threats since most of them are exposed to a public internet connection. Based on the existing studies above, this paper describes some of the key differences, benefits, and risks between on-prem file storage and cloud storage.

3. METHODOLOGY

In this study, an actual simulation of deployed cloud-based storage will be performed for a better understanding of the advantages to the organizations. The storage simulation has been divided into four phases. Phase one will focus on simulating the actual client workstations, on-premise servers, and secured cloud-based storage which is all connected to a single hosted domain, mittip.info. The storage has been configured in this phase to have auditable logs which will be used in phase two for reporting. An automated backup and backup retention policy are also set in this phase. This phase will achieve the scalability and fault tolerance of the system. Phase two is all about monitoring the health of the storage which will help the study achieve storage availability. Alarms are configured in this phase to set notifications when an anomaly has been detected. Messaging or sending communications or notifications is the focus of phase three. Topics and subscriptions are created so that notifications can be delivered through the desired communication channel. To ensure that any incidents that will occur in the system will be resolved as quickly as possible, the fourth phase will focus on incident management and help with incident logging, tracking, escalations, and resolutions.

The fifth and final phase of the experiment will focus on measuring the success of the system by conducting UAT. Multiple accounts have been created in AWS using the IAM tool. Individual testers will use each of the accounts to log in to the client workstation to test the connectivity and performance of the file server. Each account has been added to the Manila group which contains the security permissions of the cloud storage. Accounts that are created but are not members of the Manila group will not have access to the cloud storage. FSx cloud storage is mapped into the Manila group using a group policy object (GPO).

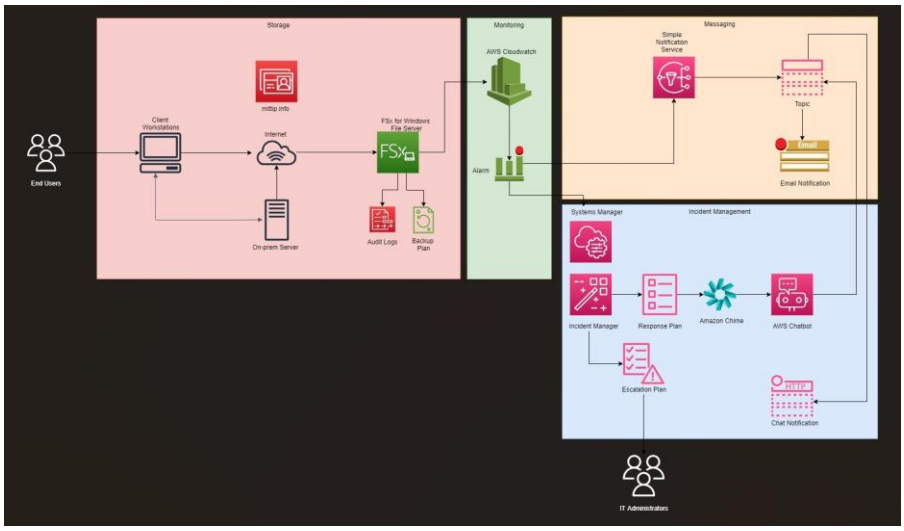

Figure 1. Proposed Cloud Storage Architecture

3.1. Storage Deployment

To address the main objective of the study, a public cloud storage deployment process has been used. The Mittip.info domain has been created to create necessary users and groups to verify the success of the study. Two elastic computing instances have been created to serve as a client and a server. The client machine will serve as a workstation while the server will be used to manage the active directory users and group policy objects which is necessary for automated mapping of the file share. FSx for Windows has been configured to serve as a file share with additional features of audit logs for enhanced security and a backup plan for data availability.

The steps below are taken in phase one:

1. A virtual private cloud (VPC) has been created in AWS to serve as a virtual network which will then be associated with other services that will be created. Subnet masks have been created in VPC to be allocated to the domain controllers, virtual machines, and file storage.
2. A domain has been created and hosted online to be used in this study. Once the domain has been hosted, it needs to be registered into the directory services offered by AWS, as shown in Figure 9. Upon creation of the domain, it needs to be associated with a VPC created in AWS.
3. Two virtual machines have been created using the EC2 services offered by AWS. One of the VMs has been created to serve as a client machine (Figure 12), and the other one has been created to serve as a physical server with additional configurations. Both VMs have been joined into the mittip.info domain.
4. Active directory accounts and group policy features are installed on the server which are both necessary to automate the mapping of the created file storage.
5. File system has been created using the FSx for Windows Server, allocating the virtual network and domain controller created earlier. An availability zone is set as well which will make the system fault-tolerant in a way that there are backup data centers in the region we have selected. KMS key ID is automatically enabled as an additional security feature that encrypts data at rest.
6. After creating the file system, it can now be attached to any devices connected to the mittip.info domain but using the command “net use \\<hostname>.<domain>\share.”

7. A user account and a security group have been created in Active Directory. The user account has been added as a member of the security group.
8. A GPO has been created and linked to the security group in the active directory. The GPO has been configured to map the file system created using the file path "\\<hostname>.<domain>\share." The file path is set to be mapped as M:\ drive from the GPO and will be mapped automatically upon the user sign-in.
9. File access auditing is an automatically enabled feature of FSx that records the logs of the file system whenever changes occur. These audit logs can be viewed in CloudWatch with a visualization.

3.2. Monitoring Storage Health

Maintaining system availability, reliability, and performance is also essential. By monitoring the storage health with the help of CloudWatch, alarms and thresholds can be configured to prevent system downtime. CloudWatch offers metrics to determine the performance of Amazon services and help detect anomaly-based events which can be configured to create alarms based on the thresholds. Events can also be configured to clean up to a much more user-friendly notification.

The steps below are taken in phase two:

1. CloudWatch has been configured in this phase. The purpose of this service is to create alarms if an anomaly has been detected. Conditions and thresholds can be set to trigger the alarm and send notifications.

2. Additional alarms are configured to monitor the data being written in the storage account. It will help determine if the storage capacity allocated is nearly full or if there are too many hosts connected to the storage at the same time.

3.3. Messaging

Monitoring server health is not useful without notifying the concerned resources to fix any anomaly experienced by the system. Messaging plays an important role in notifying the resources needed to fix any issues encountered. Topics are created in SNS which can be used as a subscription to receive notifications by concerned individuals.

The steps below are taken in phase three:

1. A Simple Notification Service topic and subscription have been created in AWS to receive notifications created by the alarms. Notifications can be in the form of email and SMS.
2. Email notifications sent through Amazon are in JavaScript object notation (JSON) format, and it will be difficult for a non-technical person to understand. For the notifications to be more precise and understandable, A JSON cleanup has been set to indicate the input path and input template when triggered through CloudWatch Events.

3.4. Incident Management

To ensure the service remains uninterrupted or to bring back any uninterrupted service as quickly as possible, an automated incident management process has been created in AWS which is connected to alarms and thresholds set by CloudWatch. Incident management helps to prevent any serious incidents that may happen in the system. With the help of response, escalation, and engagement plans, necessary IT resources can help resolve issues in the system detected by CloudWatch. CloudWatch triggers the alarm which sends a signal to the systems manager in

creating an incident ticket. Once a ticket has been created, it will perform necessary actions such as a response plan which is responsible for sending a signal to SNS to send notifications to the ones who are subscribed to the topic. It will also trigger the escalation plan and engagement plan to gather the required individuals to resolve the issue.

The steps below are taken in the final phase:

1. A response plan has been created to automate the creation of critical tickets received through the CloudWatch Alarms. The automation was enabled in AWS Systems Manager. Incident tickets will be created automatically which can easily help identify the issue.
2. An escalation plan has been created as well to escalate an incident logged to the correct support group. Additional contacts can be added as needed; durations can be configured at the time of engagement between support staff. For the contacts to be included in an escalation plan, they need to be added to the list of contacts first.
3. A chat channel and engagement have also been created. The purpose of this chat channel is to engage the selected contacts to a channel in Amazon Chime to collaborate and provide a resolution to the incident.
4. An email will be sent to the contacts once they have been engaged with an acknowledgment code they need to enter once they open the incident ticket.
5. A chatbot has been created to easily provide reports to the engaged contact in Amazon Chime, from ticket creation to ticket resolution.

4. RESULTS

A comparison between cloud storage and on-premises storage has been conducted to determine which of the storage solutions is better. Below are the key performance indicators used to measure each of the aspects discussed in the evaluation.

4.1. Costs and Maintenance

To determine the comparison of costs and maintenance of on-premise servers, this study skimmed different compute provider websites and produced an estimate of the pricing based on their recent offers for extensive server requirements of medium to large enterprises.

Alternatively, Amazon has a pricing calculator based on a consumer consumption model which allows consumers to forecast the estimated monthly costs based on the specifications and resources or services availed. Shown in Table 1 are the data gathered.

Table 1. On-prem Total Cost in 5 Years

Item	Year 1	Year 2	Year 3	Year 4	Year 5
Processor (Intel Xeon)	$813.12	$0.00	$0.00	$0.00	$0.00
64 GB RAM	$350.31	$0.00	$0.00	$0.00	$0.00
10 TB HDD	$1,169.53	$0.00	$0.00	$1,831.21	$0.00
Electricity	$9,652.61	$9,652.61	$9,652.61	$9,652.61	$9,652.61
Staffing (2 IT Staffs)	$25,958.57	$28,554.42	$31,409.86	$34,550.85	$38,005.94
Throughput Capacity	$1,375.71	$1,375.71	$1,375.71	$1,375.71	$1,375.71
Backup Storage	$813.12	$0.00	$0.00	$0.00	$0.00
Data Transfer	$0.00	$0.00	$0.00	$0.00	$0.00
Operating System	$5,797.42	$0.00	$0.00	$0.00	$0.00
Total Cost in 5 Years					$224,395.95

Table 2. Cloud Total Cost in 5 Years

Item	Year 1	Year 2	Year 3	Year 4	Year 5
Processor (Intel Xeon)	$0.00	$0.00	$0.00	$0.00	$0.00
64 GB RAM	$0.00	$0.00	$0.00	$0.00	$0.00
10 TB HDD	$1,445.77	$1,445.77	$1,445.77	$1,445.77	$1,445.77
Electricity	$0.00	$0.00	$0.00	$0.00	$0.00
Staffing (2 IT Staffs)	$12,979.28	$13,628.25	$14,309.66	$15,025.14	$15,776.40
Throughput Capacity	$5839.6	5839.6	$5839.6	$5839.6	$5839.6
Backup Storage	$0.00	$0.00	$0.00	$0.00	$0.00
Data Transfer	$271.16	$271.16	$271.16	$271.16	$271.16
Operating System	$0.00	$0.00	$0.00	$0.00	$0.00
Total Cost in 5 Years					$109,501.38

The costs calculated in an on-premise server are based on the current market value and life cycle. For example, the current market value of a server processor is $813.12 and has a life cycle of three to five years. After five years, it will no longer be supported and needs to be replaced. The same goes for the memory and hard drives. Electricity and throughput charges remain the same throughout the following years, although it is expected to increase or decrease depending on the economy. Two IT staff with a market value of $12,979 per year accumulate 5% of their yearly salary. Backup storage has the same value as the server processor since both are servers. Since the server is located locally, data transfer will not accumulate extra charges. The newest server OS released by Microsoft costs $5,797.42 and has a life cycle of 10 years.

Throughput capacity refers to the bandwidth speed for file transfers. The computation for on-premise is based on a known internet service provider in the Philippines with 200 MBps speed. Alternatively, cloud throughput capacity is determined on the initial setup of Amazon FsX which

is assessed per MBps. In this study, 200 MBps of throughput capacity only dedicated to FsX has been configured. The computation is shown below:

1 x 8 MBps per month = 8.00 MBps per month
Max (50, 8.00) = 50.00 MBps per month
200.00 MBps of provisioned throughput x 2.479 USD per MBps-month = 495.80
495.80 USD x 12 months = 5829.6 USD

Backup storage also requires upfront costs for on-premise servers since separate hardware equipment is needed for it to function as a backup server. Whereas Amazon already offers both automatic and user-initiated backup. Backup costs in AWS are determined through the hardware capacity configured. Data transfer is billed by "in" and "out" from Amazon by 0.12 USD per GB in. 200 GB of data per month would be 24 USD, unlike the on-premise in which data can be copied across different client machines or different servers on an infinite basis. The computation is shown in Tables 1 and 2.

4.2. Throughput, IOPS, and Response Time

In evaluating the storage performance, three key aspects have been thoroughly analyzed: throughput, input/output per second (IOPS), and response time. Powershell is used as a benchmarking tool to assess the performance of each storage device. Powershell is a built-in command-line-based tool included on every Windows machine.

Throughput or data transfer is measured through megabytes per second. IOPS is the measurement of storage devices on how fast read and write are performed per thread. Last, response time is determined by how fast the system will respond to the requests and is usually measured in milliseconds (ms).

In testing the different aspects of the storage performance, two testing scenarios have been done: sequential operation testing and random operation testing. Sequential operation pertains to accessing locations in a non-stop manner and is usually connected to data files of larger sizes. Random operation pertains to a non-continuous manner that is connected to smaller data files. Figure 2 and 3 show the script that runs on both on-prem and cloud storage devices. The description of the parameters used on the testing script is shown in Table 3.

```
PS C:\temp\disk_perf_iops (1)> .\DiskPerformance.ps1 -TestFileName test.dat -TestFileSiz
eInGB 1 -TestFilepath D:\ -TestMode Get-LargeIO -FastMode True -RemoveTestFile True -Out
putFormat Out-GridView
```

Figure 2. Sequential Operation Testing Script

```
PS C:\temp\disk_perf_iops (1)> .\DiskPerformance.ps1 -TestFileName test.dat -TestFileSiz
eInGB 1 -TestFilepath D:\ -TestMode Get-SmallIO -FastMode True -RemoveTestFile True -Out
putFormat Out-GridView
```

Figure 3. Random Operation Testing Script

Table 3. Powershell Script Parameters

Parameters	Description
–TestFileName	Name of the file created by the script
–TestFileSizeInGB	File size of the test data
–TestFilepath	Location of the drive that needs to be tested
–TestMode	Get-LargeIO - For large data size (sequential)
	Get-SmallIO - For small data size (random)
–FastMode	Each test runs for 10 seconds
–RemoveTestFile	Remove the test file once the script has been completed
–OutputFormat	Format of the results that will be displayed

Sequential operation testing is determined by using 512 kb of data. The results are shown below:

Table 4. Sequential Operation Testing

MB/s	**IOPS**	**Latency (ms)**	**Type**	**Target**
102.9	205.8	4	sequential	D:\\test.dat
113.01	226.03	8	sequential	D:\\test.dat
116.22	232.45	12	sequential	D:\\test.dat
113.37	226.75	17	sequential	D:\\test.dat
111.83	223.66	21	sequential	D:\\test.dat

Table 5. Sequential Cloud Testing

MB/s	**IOPS**	**Latency(ms)**	**Type**	**Target**
1192.51	2385	0	sequential	\\amznfsx0ogpdjtx.mittip.info\share\test.dat
1639.45	3278.9	0	sequential	\\amznfsx0ogpdjtx.mittip.info\share\test.dat
2150.44	4300.9	0	sequential	\\amznfsx0ogpdjtx.mittip.info\share\test.dat
2162.85	4325.7	0	sequential	\\amznfsx0ogpdjtx.mittip.info\share\test.dat
1901.54	3803.1	0	sequential	\\amznfsx0ogpdjtx.mittip.info\share\test.dat

Throughput - Based on the results gathered, data transfer speed on the cloud increased gradually with every thread, while the on-prem throughput has an unstable speed. The first thread from the cloud is 168% faster than the first thread from on-premises. The average throughput of the first 5 threads in the cloud is 1809.39 MB/s which is 177% faster compared to on-prem only gives 111.47 MB/s.

IOPS - From the data gathered, the cloud's read/write operations have a speed of 2385 IOPS during the first thread compared to 205.8 IOPS in on-prem which is 168% faster. Compared to the throughput, IOPS is not increasing gradually per thread, but the speed is maintained on both devices. The average sequential IOPS for the cloud is 3618.72, and the average sequential IOPS for on-prem is 222.9. Cloud IOPS is 177% higher than on-prem.

Response time - based on the results indicated under latency ms, on-prem storage has a four-second delay in responding to the requests which gradually increases per thread. Alternatively, cloud storage maintains system responsiveness of a zero-second delay which is better than on-prem. The average response time of the cloud is zero, while the on-prem has 12.4ms which is 200% faster. The higher the response time is, the higher the latency is experienced. Random operation testing is determined by using an 8kb file size.

Table 6. Random On-prem Testing

MB/s	IOPS	Latency (ms)	Type	Target
110.91	14197.68	1	random	D:\\test.dat
112.77	14435.67	2	random	D:\\test.dat
105.93	13559.7	2	random	D:\\test.dat
105.47	13501.09	2	random	D:\\test.dat
109.16	13972.74	2	random	D:\\test.dat

Table 7. Random Cloud Testing

MB/s	IOPS	Latency (ms)	Type	Target
191.95	24570.45	0	random	\\amznfsx0ogpdjtx.mittip.info\share\test.dat
175.75	22496.92	1	random	\\amznfsx0ogpdjtx.mittip.info\share\test.dat
168.54	21573.96	1	random	\\amznfsx0ogpdjtx.mittip.info\share\test.dat
178.61	22863.04	1	random	\\amznfsx0ogpdjtx.mittip.info\share\test.dat
166.43	21303.05	1	random	\\amznfsx0ogpdjtx.mittip.info\share\test.dat

Throughput - From the results of the data gathered, throughput can be seen with a stable transfer rate. Cloud has a transfer rate of 191.95 MB/s compared to 110.91 MB/s of on-prem during the first thread which is still 54% faster. The average transfer rate of cloud storage is 176.25 MB/s, and on-prem storage is 108.9 MB/s. The average throughput of the cloud is 47% faster than the on-prem's throughput.

IOPS - Both cloud and on-prem storage have a massive increase in random operation testing compared to sequential operation testing which is expected since the data size used in this testing

is much smaller. Cloud's IOPS during the first thread is 24570.45 compared to 14197.68 IOPS of on-prem which is 54% higher. The average cloud IOPS is 22561.48, while on-prem has only 13933.38. The average IOPS of the cloud is 47% faster than that of on-prem IOPS.

Response Time - Results from the data gathered in random operational testing show that the latency of on-prem gradually decreased compared to the sequential operation testing, while the cloud's response time has increased a bit but is still faster compared to on-prem. The latency experienced through the first 5 threads of on-prem ranges from 1-2ms, while on cloud, it ranges from 0-1ms. The average latency of the cloud is 0.8ms compared to 1.8ms of on-prem which is 77% higher.

4.3. Incident Management

Table 8. On-prem Incident Management (Manual)

Created	Date Closed	Engagement Time	MTBE
08/06/2022 19:35	13/06/2022 21:00	10/06/2022 19:41	2 days, 00 hours, 05 minutes, and 56 seconds
12/06/2022 12:55	17/06/2022 15:00	13/06/2022 13:11	1 day, 00 hours, 16 minutes, and 19 seconds
11/06/2022 13:45	16/06/2022 16:00	12/06/2022 13:46	1 day, 00 hours, 00 minutes, and 34 seconds
07/06/2022 22:40	21/06/2022 17:01	07/06/2022 23:21	0 day, 00 hours, 41 minutes, and 00 seconds
09/06/2022 1:33	14/06/2022 4:00	10/06/2022 2:07	1 day, 00 hours, 33 minutes, and 24 seconds

Table 9. Cloud Incident Management

Created	Date Closed	Engagement Time	MTBE
17/03/2022 0:23	2022-03-18 00:26:40	17/03/2022 0:23	0 days, 00 hours, 0 minutes, and 0 seconds
07/06/2022 20:27	2022-06-07 20:41:34	07/06/2022 20:27	0 days, 00 hours, 0 minutes, and 1 seconds
08/06/2022 20:05	2022-06-08 20:09:41	08/06/2022 20:05	0 days, 0 hours, 0 minutes, and 1 seconds
08/06/2022 20:53	2022-06-08 20:58:40	08/06/2022 20:53	0 days, 0 hours, 0 minutes, and 1 seconds
17/06/2022 8:26	2022-06-17 08:27:31	17/06/2022 8:26	0 days, 0 hours, 0 minutes, and 11 seconds

Mean time between engagement (MTBE) is measured between the time the ticket has been lodged and the acknowledgment of the support team. Incident age is determined between the time of incident creation and the resolution. The results show that an automated incident management approach can help close the gap of manual engagement of necessary staff to address the issues of an incident.

4.4. User Acceptance Testing

To determine the success of the system, UAT has been implemented to gather feedback from existing users of file servers. Each of the users who participated has tested if they can perform their day-to-day tasks in the file server. The questions are basically to perform add, edit, transfer, and delete files on the cloud storage. They were also given a chance to rate the performance of the cloud storage to the existing file server they are using. The testing is categorized into two different areas: the client machine and the cloud storage.

The results from the testing validated that users could perform their day-to-day tasks using AWS, and they are rating it better than the current file server they are using.

5. CONCLUSION

A comparison between cloud storage and the traditional on-premise file server has been made in this study. Different aspects of both storages have been thoroughly analyzed, including cost, maintenance, performance, and incident management. Since the cloud removes the upfront costs (CaPex) and only provides operational costs (OpEX), the results from cost and maintenance proved that the cloud offers a much more cost-efficient service compared to on-prem in the span of 5 years.

Performance data are gathered on two different kinds of testing: random operational testing and sequential operational testing. Throughput, IOPS, and response time are the performance counters measured which have been evaluated using a benchmarking tool. Based on the results of the testing, the cloud's throughput, IOPS, and response time are better compared to on-prem.

Automated incident tracking and manual incident tracking have been evaluated as well based on the actual incident tracking tool for on-prem and a simulated incident tracking tool in the cloud. The results show that by using an automated incident tracking tool, the engagement time between the system issue and the support can be lessened which can result in a faster resolution of issues. Last, testing based on end-users perspectives has been conducted to evaluate the cloud storage as a replacement for on-prem, where the users have concluded that the performance is better in the cloud.

Overall, given the results from the various aspects of thorough research and testing. Companies may find cloud storage beneficial compared to on-prem storage. It is more cost-efficient, easy to maintain, delivers better performance, provides enhanced availability with the help of automated incident management, and is user-friendly.

REFERENCES

[1] D. Tapscott and A. Caston, “Paradigm shift : the new promise of information technology,” p. 337.

[2] S. V. Aleksandrova, M. N. Aleksandrov, and V. A. Vasiliev, “Business Continuity Management System,” Proc. 2018 Int. Conf. ’ ’Quality Manag. Transp. Inf. Secure. Inf. Technol. IT QM IS 2018, pp. 14–17, Nov. 2018, doi: 10.1109/ITMQIS.2018.8525111.

[3] R. Gyorodi, M. I. Pavel, C. Gyorodi, and D. Zmaranda, “Performance of OnPrem Versus Azure SQL Server: A Case Study,” IEEE Access, vol. 7, pp. 15894–15902, 2019, doi: 10.1109/ACCESS.2019.2893333.

[4] M. F. Flores, “Understanding The Challenges Of Remote Working And Its Impact To Workers,” Int. J. Bus. Mark. Manag., vol. 4, no. 11, pp. 40–44, 2019.

[5] C. Study, B. Network, S. Provider, and A. I. Prioritization, “Designing Supervised Learning-Based Incident Management Model,” 2019.

[6] E. Lavrov, P. Paderno, O. Siryk, E. Burkov, N. Pasko, and V. Nahornyi, “Decision Support in Incident Management Systems. Models of Searching for Ergonomic Reserves to Increase Efficiency,” 2020 IEEE Int. Conf. Probl. Infocommunications Sci. Technol. PIC S T 2020 - Proc., pp. 653–658, 2021, doi: 10.1109/PICST51311.2020.9467991.

[7] M. Lim, “C2CFTP: Direct and Indirect File Transfer Protocols between Clients in Client-Server Architecture,” IEEE Access, vol. 8, pp. 102833–102845, 2020, doi: 10.1109/ACCESS.2020.2998725.

[8] K. Namee, S. Karnbunjong, and J. Polpinij, “The Integration of File Server Function and Task Management Function to Replace Web Application on Cloud Platform for Cost Reduction,” Proc. - APCCAS 2019 2019 IEEE Asia Pacific Conf. Circuits Syst. Innov. CAS Towar. Sustain. Energy Technol. Disrupt., pp. 405–408, 2019, doi: 10.1109/APCCAS47518.2019.8953164.

[9] J. Liu, A. C. Arpaci-Dusseau, R. H. Arpaci-Dusseau, and S. Kannan, “File systems as processes,” 11th USENIX Work. Hot Top. Storage File Syst. HotStorage 2019, co-located with USENIX ATC 2019, 2019.

[10] J. Pablo, C. J. Pajigal, C. Palileo, and E. Blancaflor, “Developing a Web-based Water Incident Management System with Decision Support,” 2020 IEEE 7th Int. Conf. Ind. Eng. Appl. ICIEA 2020, pp. 519–524, 2020, doi: 10.1109/ICIEA49774.2020.9101965.

[11] C. Ebert, C. Henrique, and C. Duarte, “Digital Transformation The Influence of Regulatory Requirements on ICT Businesses View project,” 2018, doi: 10.1109/MS.2018.2801537.

[12] D. Kolevski, K. Michael, and M. Freeman, “Cloud c omputing d ata b reaches : A r eview of U . S . r regulation and d ata b reach n notification l iterature,” 2021.

AUTHORS

Jaymie Rae Medina

An IT professional who specializes in end-user support and compute services. He is currently taking his Masters in Information Technology in Technological Institute of the Philippines. He also holds various industry certificates such as ITIL, Lean Six Sigma Yellow Belt, Microsoft Certified Professional, and Azure Fundamentals.

Jennalyn Mindoro

A Computer Engineering professor at the Technological Institute of the Philippines. She completed her PhD in Engineering last 2016 in TIP.